UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,987	11/08/2000	Richard Schroeppel	2944.2.1	5823

7590 03/07/2006

Richard Schroeppel
500 S. Maple Drive
Woodland Hills,, UT 84653

EXAMINER	
DADA, BEEMNET W	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/710,987	SCHROEPPEL, RICHARD	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37 and 42-59* is/are rejected.

7)☐ Claim(s) *38-41* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on December 05, 2005. Claims 1, 29 and 59 have been amended. Claims 1-59 are pending.

Response to Arguments

2. Applicant's arguments filed December 05, 2005, with respect to 35 U.S.C. 103 (a) rejection of claims 38-41 over Vanstone in view of Koyama and further in view of Elkies have been fully considered and are persuasive. The rejection of claims 38-41 has been withdrawn.

3. Applicant's arguments with respect to 35 U.S.C. 103(a) rejection of claims 1-37 and 42-59 over Vanstone in view of Koyama have been fully considered but they are not persuasive. Applicant argues that Vanstone and Koyama cannot be combined, both references discuss elliptic curve cryptosystem, however, in the method of Koyama, the orders of the elliptic curves are generally independent of some of the coefficients in the curve equations, which is different from the Vanstone system. Applicant further argued that Koyama's halving algorithm only woks for the particular primes described it the Koyama reference and doesn't apply to prime power finite fields such as the one described in Vanstone. Examiner disagrees.

4. Examiner would point out that, In response to applicant's argument that Vanstone and Koyama cannot be logically combined, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In this case Koyama discloses the use of halving algorithm in elliptic curve cryptosystem.

Employing the overall concept of using halving algorithm in elliptic curve algorithm as taught by Koyama within the elliptic curve cryptosystem of Vanstone teaches the claimed limitations. Examiner asserts that the art on record teaches the claimed limitation and therefore the rejection is respectfully maintained.

Allowable Subject Matter

5. Claims 38-41are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-37 and 42-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. US Patent 6,141,420 (hereinafter referred as Vanstone) in view of Koyama et al. Elliptic Curve Cryptosystems and Their Applications (hereinafter Koyama).

8. As per claim 1, Vanstone teaches a method comprising:

selecting an elliptic curve method [column 2, lines 60-63];

executing a point modification algorithm to manipulate points of the elliptic curve method [column 2, lines 35-43];

generating a signal having a distinct characteristic (i.e. generating an encryption key) using the selected elliptic curve method [column 2, lines 65-67 & column 3, lines 1-11];

providing substantive content (i.e. sending / receiving a message) [column 2, lines 60-63]; and

manipulating the substantive content (i.e. encrypting/decrypting) using the distinct characteristic [column 3, lines 12-13].

Vanstone is silent on point modification algorithm that includes at least one occurrence of point fractioning. Koyama teaches an Elliptic curve cryptosystem including a point modification algorithm that includes at least on occurrence of point fractioning (halving algorithm) [see, pages 52-53, section 2.3 Halving algorithm]. Both Vanstone and Koyama teach an elliptic curve cryptosystem. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Koyama within the system of Vanstone in order to efficiently process elliptic cryptosystem (see, page 53, Theorem 5, polynomial time algorithm).

9. As per claims 26 and 29, Vanstone teaches an apparatus comprising:

a system for creating a distinct characteristic configured to support cryptographic manipulation of information [column 8, lines 20-25];

a memory device operably connected to the system for storing the distinct characteristic and executables programmed to operate on the distinct characteristic [column 8, lines 55-60];

an encrypting device operably connected to the system for controlling an encryption process using the distinct characteristic [column 8, lines 60-67];

the system further configured to execute an elliptic curve method for generating the distinct characteristic [column 2, lines 60-63]; and

the system further configured to execute a point modification algorithm for generating the distinct characteristic [column 2, lines 35-43].

Vanstone is silent on point modification algorithm that includes at least one occurrence of point fractioning. Koyama teaches an Elliptic curve cryptosystem including a point modification algorithm that includes at least on occurrence of point fractioning (halving algorithm) [see, pages 52-53, section 2.3 Halving algorithm]. Both Vanstone and Koyama teach an elliptic curve cryptosystem. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Koyama within the system of Vanstone in order to efficiently process elliptic cryptosystem (see, page 53, Theorem 5, polynomial time algorithm).

10. As per claim 59, Vanstone teaches a method comprising:

selecting an elliptic curve method [column 2, lines 60-63];

executing a point modification algorithm to manipulate points of the elliptic curve method [column 2, lines 35-43];

generating a signal having a distinct characteristic (i.e. generating an encryption key) using the selected elliptic curve method [column 2, lines 65-67 & column 3, lines 1-11];

providing substantive content (i.e. sending / receiving a message) [column 2, lines 60-63]; and

manipulating the substantive content (i.e. encrypting/decrypting) using the distinct characteristic [column 3, lines 12-13].

Vanstone is silent on point modification algorithm comprising one or more ambiguous point triplications steps, where the ambiguity is resolved by determining whether a point is twice halvable. Koyama teaches an Elliptic curve point modification algorithm comprising one or more ambiguous point triplications steps, where the ambiguity is resolved by determining whether a point is twice halvable [see, pages 52-53, section 2.3 Halving algorithm]. Both Vanstone and Koyama teach an elliptic curve cryptosystem. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Koyama within the system of Vanstone in order to efficiently process elliptic cryptosystem (see, page 53, Theorem 5, polynomial time algorithm).

11. As per claims 2, 27, and 30, Vanstone teaches the method/apparatus as applied to claims 1, 26 and 30 above. Furthermore Vanstone teaches the method/apparatus, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof [column 4, lines 55-57, column 3, lines 56-64, column 10, line 61].

12. As per claims 3 and 4, Vanstone further teaches the method, wherein manipulating the substantive content comprises encrypting / decrypting the substantive content [column 3, lines 12-13 and column 3, lines 19-20].

13. As per claims 8, and 33, Vanstone further teaches the method further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance (generating a session key randomly during a session) [column 3, lines 1-15].

14. As per claim 13, Vanstone further teaches the method, further comprising selecting a first point and pre-modifying (in a predetermined method) the first point by a modification operation configured to compensate for some of the processing steps, added and corresponding to execution of a series of steps in accordance with the method [column 5, lines 56-67].

15. As per claim 14, Vanstone further teaches the method, further comprising sending by a sender and receiving by a receiver the substantive content, and wherein the sender executes a first operation during modification for encryption and the receiver executes a second and distinct operation during modification for decryption [column 2, lines 60-67 and column 3, lines 1-24].

16. As per claims 5, 15 and 35, Vanstone further teaches the method, wherein generating the distinct characteristic further comprises creating a distinct characteristic selected from a symmetric key configured to be shared by two or more parties, a decryption code for processing an encrypted signal, a digital signature, an asymmetric key, and an authentication (i.e. public/private keys used for encryption/decryption, authentication and a shared session key used for encryption/decryption) [column 3, lines 1-24].

17. As per claim 16, Vanstone further teaches the method, further comprising selecting a point and wherein the point is of a type selected from a hyperelliptic curve, an algebraic curve, and abelian variety [column 3, lines 49-56].

18. As per claim 28, Vanstone further teaches the apparatus, wherein the distinct characteristic is configured to be processable by the system for divulging independently to two independent parties a secret to be shared by the two independent parties [column 3, lines 9-15].

19. As per claim 36, Vanstone further teaches the method, wherein the elliptic curve is over a finite field [column 2, lines 27-32]; the finite field is represented by a field polynomial [column 2, lines 29-30]; and the field polynomial is of low hamming weight [column 13, lines 60-62].

20. As per claim 37, Vanstone further teaches the method, wherein the field polynomial is selected form a binomial, a trinomial, and a pentanomial (i.e. polynomials of degree 2, 3, and 5) [column 8, lines 39-41, and column 6, lines 30-32].

21. As per claim 42, and 53-55, Vanstone further teaches the method, wherein the point modification algorithm comprises solving a quadratic equation using efficient algorithm [column 20, claim 32, and column 21, claims 39 & 40].

22. As per claim 43, Vanstone further teaches the method, wherein the point modification algorithm comprises computing a reciprocal (multiplicative inverse) of a field element using efficient algorithm [column 11, lines 39-42].

23. As per claim 44, Vanstone further teaches the method, wherein the point modification algorithm comprises at least one of adding and subtracting of elliptic curve points using efficient algorithm [column 12, lines 35-41].

24. As per claim 45, Vanstone further teaches the method wherein the addition and subtraction comprises computing a reciprocal of a field element using an efficient algorithm [column 15, lines 56-67 and column 16, lines 1-16].

25. As per claim 49, Vanstone further teaches the method, wherein the point modification algorithm further comprises choosing a multiplier having a low hamming weight [column 13, lines 60-62].

26. As per claim 50, Vanstone further teaches the method, wherein the point modification algorithm includes point addition and subtraction steps and the point modification algorithm is chosen to minimize the number of steps [column 3, lines 56-62 and column 4, lines 49-65].

27. As per claims 47, 48 and 51, Vanstone further teaches the method, wherein the point modification algorithm is an addition-subtraction chain intermixed with point fractioning [column 4, lines 7-25].

28. As per claim 52, Vanstone further teaches the method, wherein the elliptic curve is over a finite field, and the size of the finite field is increased such that a smaller number of addition and subtraction steps may be combined with a larger number of point fractioning steps, such that the overall computation effort is reduced, while preserving a specified level of security [column 4, lines 7-63].

29. As per claims 56-58, Vanstone further teaches the method, wherein the modification algorithm further comprises:

using plurality of representations of the points, using input points in one or more representations to produce output points in a different representation wherein at least three changes of representation occur [column 15, lines 51-65 and column 16, lines 1-20].

30. As per claims 6, 7, 21, 31 and 32, Vanstone further teaches executing modification algorithm to manipulate points of the elliptic curve method [column 2, lines 35-43]. Vanstone also teaches modification algorithms selected form point multiplying, point fractioning [column 4, lines 55-57, column 3, lines 56-64, column 10, line 61]. Koyama teaches modification algorithm wherein point fraction is selected from integral point fractioning, corresponding to a denominator that is an integral number [see, pages 52-53, section 2.3 Halving algorithm].

31. As per claims 9, 10 and 34, Vanstone further teaches the method/apparatus further comprising selecting a first point for execution of the point modification algorithm, based on a selected property [column 2, lines 27-31 and lines 39-43].

32. As per claims 11 and 12, Vanstone further teaches the method further comprising repeating the point modification algorithm with second point selected by another entity selected from deterministic process, a random process, and a third party [column 3, lines 17-23]; wherein the second point is communicated to the point modification in a format from a message and certificate [column 3, lines 14-15].

33. As per claims 17-20, 22-25, and 46, Vanstone further teaches point represented in Cartesian space and point existing in a mapped Cartesian space having Cartesian representation (i.e. a point P represented as P(x,y) (x coordinate, y coordinate) [column 2, lines

60-62]. Vanstone also teaches point multiplication in a finite group whose member lie on an elliptic curve [column 2, lines 27-30 and column 4, lines 55-58. Koyama teaches elliptic curve cryptosystem including point-halving operations [see, pages 52-53, section 2.3 Halving algorithm].

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

February 15, 2006

HOSUK SONG
PRIMARY EXAMINER